

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 comparing first security level information and second security level
3 information, wherein
4 said first security level information is stored in a security label of a
5 packet received at a network node, and
6 said second security level information is stored at said network node;
7 and
8 indicating processing to be performed on said packet based on said comparing.

- 1 2. The method of claim 1, wherein
2 said first security level information represents a first security level, and
3 said second security level information represents a second security level.

- 1 3. The method of claim 2, wherein
2 said first security level and said second security level implement one of a
3 multi-level security paradigm and a multi-lateral security paradigm.

- 1 4. The method of claim 2, wherein
2 said security label is one of an enumerated security label and a bitmap security
3 label.

- 1 5. The method of claim 2, wherein
2 said second security level is a security level of a port of said network node.

- 1 6. The method of claim 5, further comprising:
2 setting said security level of said port.

- 1 7. The method of claim 6, wherein said setting said security level of said
2 port comprises:
3 storing said second security level in a security label information field of an
4 access control list entry.

1 8. The method of claim 6, wherein said setting said security level of said
2 port comprises:

3 storing said second security level in a label range information field of a
4 forwarding table entry.

1 9. The method of claim 2, wherein said processing comprises:
2 dropping said packet, if said comparing indicates that said first security level is
3 less than said second security level.

1 10. The method of claim 2, wherein
2 said processing comprises at least one of dropping said packet, redirecting said
3 packet and rewriting said security label.

1 11. The method of claim 1, wherein
2 said first security level information represents a first security level, and
3 said second security level information represents a plurality of security levels.

1 12 The method of claim 11, wherein
2 said security levels are a range of security levels.

1 13 The method of claim 12, wherein said processing comprises:
2 dropping said packet, if said comparing indicates that said first security level is
3 not within said range of security levels.

1 14. The method of claim 1, further comprising:
2 storing said second security level information at said network node.

1 15. The method of claim 14, wherein said storing comprises:
2 storing said second security level in a security label information field of an
3 access control list entry.

- 1 16. The method of claim 14, wherein said storing comprises:
2 storing said second security level in a label range information field of a
3 forwarding table entry.

- 1 17. The method of claim 14, wherein said storing comprises:
2 communicating said second security level from a first network node by
3 registering said second security level in a context.

- 1 18. The method of claim 17, wherein said registering comprises:
2 updating said second security level information by logically OR'ing third
3 security level information with said second security level information.

- 1 19. The method of claim 17, wherein
2 said context is a generic attribute registration protocol information propagation
3 context, and
4 said registering said second security level is accomplished by said first
5 network node issuing a join request.

- 1 20. The method of claim 14, wherein said storing comprises:
2 storing said second security level in a label range information field of
3 forwarding table.

- 1 21. The method of claim 14, wherein said storing comprises:
2 storing said second security level in a port of said network node.

- 1 22. The method of claim 21, wherein
2 said port is an egress port.

- 1 23. The method of claim 2, further comprising:
2 determining said first security level.

- 1 24. The method of claim 23, wherein said determining comprises:
2 determining if an ingress port is marked as an access port; and

3 setting a security level of said ingress port to said first security level, if said
4 ingress port is marked as an access port.

1 25. The method of claim 24, further comprising:
2 setting said first security level information to said security level of said ingress
3 port.

1 26. The method of claim 23, further comprising:
2 authenticating a user having said first security level, wherein
3 said determining is performed only if said user is authenticated.

1 27. The method of claim 2, further comprising:
2 performing said processing on said packet based on said comparing.

1 28. The method of claim 27, wherein said performing said processing
2 comprises:
3 forwarding said packet, if said indicating indicates that said packet is allowed
4 to be forwarded; and
5 dropping said packet, otherwise.

1 29. The method of claim 27, wherein said performing said processing
2 comprises:
3 forwarding said packet to a firewall, if said indicating indicates that said
4 packet should be forwarded to said firewall.

1 30. The method of claim 2, further comprising:
2 stripping network security information from said packet; and
3 adding subnetwork security information to said packet.

1 31. The method of claim 30, wherein
2 said network security information comprises said first security level
3 information.

1 32. The method of claim 30, wherein
2 said subnetwork security information comprises said first security level
3 information.

1 33. A computer system comprising:
2 a processor;
3 computer readable medium coupled to said processor; and
4 computer code, encoded in said computer readable medium, configured to
5 cause said processor to:
6 compare first security level information and second security level
7 information, wherein
8 said first security level information is stored in a security label
9 of a packet received at a network node, and
10 said second security level information is stored at said network
11 node; and
12 indicate processing to be performed on said packet based on said
13 comparing.

1 34. The computer system of claim 33, wherein
2 said first security level information represents a first security level, and
3 said second security level information represents a second security level.

1 35. The computer system of claim 34, wherein said computer code is
2 further configured to cause said processor to:
3 set said security level of a port, wherein
4 said second security level is a security level of said port of said
5 network node.

1 36. The computer system of claim 35, wherein said computer code
2 configured to cause said processor to set said security level of said port is further
3 configured to cause said processor to:

4 store said second security level in a security label information field of an
5 access control list entry.

1 37. The computer system of claim 35, wherein said computer code
2 configured to cause said processor to set said security level of said port is further
3 configured to cause said processor to:

4 store said second security level in a label range information field of a
5 forwarding table entry.

1 38. The computer system of claim 33, wherein
2 said first security level information represents a first security level, and
3 said second security level information represents a plurality of security levels.

1 39. The computer system of claim 33, wherein said computer code is
2 further configured to cause said processor to:
3 store said second security level information at said network node.

1 40. The computer system of claim 39, wherein said computer code
2 configured to cause said processor to store is further configured to cause said
3 processor to:

4 store said second security level in a security label information field of an
5 access control list entry.

1 41. The computer system of claim 39, wherein said computer code
2 configured to cause said processor to store is further configured to cause said
3 processor to:

4 store said second security level in a label range information field of a
5 forwarding table entry.

1 42. The computer system of claim 39, wherein said computer code
2 configured to cause said processor to store is further configured to cause said
3 processor to:

4 communicate said second security level from a first network node by virtue of
5 being configured to cause said processor to register said second security
6 level in a context.

1 43. The computer system of claim 42, wherein said computer code
2 configured to cause said processor to register is further configured to cause said
3 processor to:

4 update said second security level information by virtue of being configured to
5 cause said processor to logically OR third security level information
6 with said second security level information.

1 44. The computer system of claim 43, wherein
2 said context is a generic attribute registration protocol information propagation
3 context, and

4 said computer code configured to cause said processor to register said second
5 security level is configured to cause said processor to cause said first
6 network node to issue a join request.

1 45. The computer system of claim 34, wherein said computer code is
2 further configured to cause said processor to:
3 determine said first security level.

1 46. The computer system of claim 45, wherein said computer code is
2 further configured to cause said processor to:
3 authenticate a user having said first security level, wherein
4 said computer code configured to cause said processor to determine
5 said first security level causes said processor to determine said
6 first security level only if said user is authenticated.

1 47. The computer system of claim 45, wherein said computer code
2 configured to cause said processor to determine said first security level is further
3 configured to cause said processor to:

4 determine if an ingress port is marked as an access port; and
5 set a security level of said ingress port to said first security level, if said ingress
6 port is marked as an access port.

1 48. The computer system of claim 47, wherein said computer code is
2 further configured to cause said processor to:

3 set said first security level information to said security level of said ingress
4 port.

1 49. The computer system of claim 34, wherein said computer code is
2 further configured to cause said processor to:

3 perform said processing on said packet based on a result generated by said
4 computer code configured to cause said processor to compare.

1 50. The computer system of claim 49, wherein said computer code
2 configured to cause said processor to perform said processing on said packet is further
3 configured to cause said processor to:

4 forward said packet, if said computer code configured to cause said processor
5 to indicate indicates that said packet is allowed to be forwarded; and
6 drop said packet, otherwise.

1 51. The computer system of claim 34, wherein said computer code is
2 further configured to cause said processor to:

3 strip network security information from said packet; and
4 add subnetwork security information to said packet.

1 52. A computer program product comprising:
2 a first set of instructions, executable on a computer system, configured to
3 compare first security level information and second security level
4 information, wherein
5 said first security level information is stored in a security label of a
6 packet received at a network node, and
7 said second security level information is stored at said network node;
8 and
9 a second set of instructions, executable on said computer system, configured to
10 indicate processing to be performed on said packet based on said
11 comparing; and
12 computer readable media, wherein said computer program product is encoded
13 in said computer readable media.

1 53. The computer program product of claim 52, wherein
2 said first security level information represents a first security level, and
3 said second security level information represents a second security level.

1 54. The computer program product of claim 53, further comprising:
2 a third set of instructions, executable on said computer system, configured to
3 set said security level of a port, wherein
4 said second security level is a security level of said port of said
5 network node.

1 55. The computer program product of claim 54, wherein said third set of
2 instructions comprises:
3 a first subset of instructions, executable on said computer system, configured
4 to store said second security level in a security label information field
5 of an access control list entry.

1 56. The computer program product of claim 54, wherein said third set of
2 instructions comprises:

3 a first subset of instructions, executable on said computer system, configured
4 to store said second security level in a label range information field of a
5 forwarding table entry.

1 57. The computer program product of claim 52, wherein
2 said first security level information represents a first security level, and
3 said second security level information represents a plurality of security levels.

1 58. The computer program product of claim 52, further comprising:
2 a third set of instructions, executable on said computer system, configured to
3 store said second security level information at said network node.

1 59. The computer program product of claim 58, wherein said third set of
2 instructions comprises:
3 a first subset of instructions, executable on said computer system, configured
4 to store said second security level in a security label information field
5 of an access control list entry.

1 60. The computer program product of claim 58, wherein said third set of
2 instructions comprises:
3 a first subset of instructions, executable on said computer system, configured
4 to store said second security level in a label range information field of a
5 forwarding table entry.

1 61. The computer program product of claim 58, wherein said third set of
2 instructions comprises:
3 a first subset of instructions, executable on said computer system, configured
4 to communicate said second security level from a first network node
5 comprises a first sub-subset of instructions, executable on said

6 computer system, configured to cause said processor to register said
7 second security level in a context.

1 62. The computer program product of claim 61, wherein said first sub-
2 subset of instructions comprises:

3 a first sub-sub-subset of instructions, executable on said computer system,
4 configured to update said second security level information comprises
5 a first sub-sub-subset of instructions, executable on said computer
6 system configure to cause said processor to logically OR third security
7 level information with said second security level information.

1 63. The computer program product of claim 62, wherein
2 said context is a generic attribute registration protocol information propagation
3 context, and
4 said first sub-subset of instructions is further configured to cause said first
5 network node to issue a join request.

1 64. The computer program product of claim 53, further comprising:
2 a third set of instructions, executable on said computer system, configured to
3 determine said first security level.

1 65. The computer program product of claim 64, further comprising:
2 a fourth set of instructions, executable on said computer system, configured to
3 authenticate a user having said first security level, wherein
4 said third set of instructions is further configured to cause said
5 processor to determine said first security level only if said user
6 is authenticated.

1 66. The computer program product of claim 64, wherein said third set of
2 instructions comprises:
3 a first subset of instructions, executable on said computer system, configured
4 to determine if an ingress port is marked as an access port; and

5 a second subset of instructions, executable on said computer system,
6 configured to set a security level of said ingress port to said first
7 security level, if said ingress port is marked as an access port.

1 67. The computer program product of claim 66, further comprising:
2 a fifth set of instructions, executable on said computer system, configured to
3 set said first security level information to said security level of said
4 ingress port.

1 68. The computer program product of claim 53, further comprising:
2 a third set of instructions, executable on said computer system, configured to
3 perform said processing on said packet based on a result generated by
4 said first set of instructions.

1 69. The computer program product of claim 68, wherein said third set of
2 instructions comprises:

3 a first subset of instructions, executable on said computer system, configured
4 to forward said packet, if said second set of instructions indicates that
5 said packet is allowed to be forwarded; and
6 a second subset of instructions, executable on said computer system,
7 configured to drop said packet, otherwise.

1 70. The computer program product of claim 53, further comprising:
2 a third set of instructions, executable on said computer system, configured to
3 strip network security information from said packet; and
4 a fourth set of instructions, executable on said computer system, configured to
5 add subnetwork security information to said packet.

1 71. An apparatus comprising:
2 means for comparing first security level information and second security level
3 information, wherein
4 said first security level information is stored in a security label of a
5 packet received at a network node, and

6 said second security level information is stored at said network node;
7 and
8 means for indicating processing to be performed on said packet based on said
9 comparing.

1 72. The apparatus of claim 71, wherein
2 said first security level information represents a first security level, and
3 said second security level information represents a second security level.

1 73. The apparatus of claim 72, further comprising:
2 means for setting said security level of a port, wherein
3 said second security level is a security level of said port of said
4 network node.

1 74. The apparatus of claim 73, wherein said means for setting said security
2 level of said port comprises:
3 means for storing said second security level in a security label information
4 field of an access control list entry.

1 75. The apparatus of claim 73, wherein said means for setting said security
2 level of said port comprises:
3 means for storing said second security level in a label range information field
4 of a forwarding table entry.

1 76. The apparatus of claim 71, wherein
2 said first security level information represents a first security level, and
3 said second security level information represents a plurality of security levels.

1 77. The apparatus of claim 71, further comprising:
2 means for storing said second security level information at said network node.

1 78. The apparatus of claim 77, wherein said means for storing comprises:
2 means for storing said second security level in a security label information
3 field of an access control list entry.

1 79. The apparatus of claim 77, wherein said means for storing comprises:
2 means for storing said second security level in a label range information field
3 of a forwarding table entry.

1 80. The apparatus of claim 77, wherein said means for storing comprises:
2 means for communicating said second security level from a first network node
3 comprising means for registering said second security level in a
4 context.

1 81. The apparatus of claim 80, wherein said means for registering
2 comprises:
3 means for updating said second security level information comprising means
4 for logically OR'ing third security level information with said second
5 security level information.

1 82. The apparatus of claim 81, wherein
2 said context is a generic attribute registration protocol information propagation
3 context, and
4 said means for registering said second security level comprises means for
5 causing said first network node to issue a join request.

1 83. The apparatus of claim 72, further comprising:
2 means for determining said first security level.

1 84. The apparatus of claim 83, further comprising:
2 means for authenticating a user having said first security level, wherein
3 said means for determining is performed only if said user is
4 authenticated.

1 85. The apparatus of claim 83, wherein said means for determining
2 comprises:
3 means for determining if an ingress port is marked as an access port; and
4 means for setting a security level of said ingress port to said first security level,
5 if said ingress port is marked as an access port.

1 86. The apparatus of claim 85, further comprising:
2 means for setting said first security level information to said security level of
3 said ingress port.

1 87. The apparatus of claim 72, further comprising:
2 means for performing said processing on said packet, wherein said means for
3 performing said processing uses a result generated by said means for
4 comparing.

1 88. The apparatus of claim 87, wherein said performing said means for
2 processing comprises:
3 means for forwarding said packet, if said means for indicating indicates that
4 said packet is allowed to be forwarded; and
5 means for dropping said packet, otherwise.

1 89. The apparatus of claim 72, further comprising:
2 means for stripping network security information from said packet; and
3 means for adding subnetwork security information to said packet.

1 90. A network device comprising:
2 a network interface, wherein
3 said network interface is configured to receive a packet, and
4 said network device is configured to store first security level
5 information and to process said packet using said first security
6 level information.

1 91. The network device of claim 90, wherein
2 said network interface comprises a port, and
3 said port is configured to store said first security level information.

1 92. The network device of claim 91, wherein
2 said port is an egress port.

1 93. The network device of claim 91, wherein
2 said network device is further configured to set a security level of said port.

1 94. The network device of claim 90, wherein
2 said network device is further configured to
3 compare said first security level information and second security level
4 information, wherein
5 said second security level information is stored in a security
6 label of a packet received at said network device; and
7 indicate processing to be performed on said packet based on said
8 comparing.

1 95. The network device of claim 94, wherein
2 said second security level information represents a second security level, and
3 said first security level information represents a first security level.

1 96. The network device of claim 95, wherein
2 said network device is further configured to process said packet based on said
3 comparing.

1 97. The network device of claim 95, wherein
2 said network device is further configured to strip network security information
3 from said packet and add subnetwork security information to said
4 packet.

- 1 98. The network device of claim 95, wherein
- 2 said first security level is a security level of a port of said network device.

- 1 99. The network device of claim 94, wherein
- 2 said second security level information represents a second security level, and
- 3 said first security level information represents a plurality of security levels.

- 1 100 The network device of claim 99, wherein
- 2 said security levels are a range of security levels.

- 1 101. The network device of claim 95, wherein
- 2 said network device is further configured to store said first security level
- 3 information at said network device.

- 1 102. The network device of claim 101, wherein
- 2 said network device is further configured to communicate said first security
- 3 level from a second network device by registering said first security
- 4 level in a context.

- 1 103. The network device of claim 102, wherein
- 2 said context is a generic attribute registration protocol information propagation
- 3 context, and
- 4 said registering said first security level is accomplished by said second
- 5 network device issuing a join request.

- 1 104. A network device comprising:
- 2 an access control list, wherein
- 3 said access control list comprises an access control list entry,
- 4 said access control list entry comprises a label information field, and
- 5 said label information field is configured to store a security label.

- 1 105. The network device of claim 104, wherein
- 2 said security label implements a multi-level security paradigm.

1 106. The network device of claim 104, wherein
2 said security label implements a multi-lateral security paradigm.

1 107. The network device of claim 104, wherein said access control list entry
2 further comprises:

3 a flow label field, wherein
4 said flow label field allows said access control list entry to be identified
5 as a security labeled access control list entry.

1 108. The network device of claim 107, wherein said access control list entry
2 further comprises:

3 a plurality of flow specification fields, wherein
4 said flow specification fields comprise information identifying
5 processing to be performed on at least one flow.

1 109. The network device of claim 104, wherein
2 said security label is configured to be compared to a security label of a packet.

1 110. The network device of claim 109, wherein said access control list entry
2 further comprises:

3 a flow specification field, wherein
4 said flow specification field comprise information identifying
5 processing to be performed on said packet.

1 111. The network device of claim 110, wherein said access control list entry
2 further comprises:

3 a flow label field, wherein
4 said flow label field allows said access control list entry to be identified
5 as a security labeled access control list entry.

1 112. A network device comprising:
2 a forwarding table, wherein

3 said forwarding table comprises a plurality of forwarding table entries,
4 and
5 at least one forwarding table entry of said forwarding table entries
6 comprises a label range field.

1 113. The network device of claim 112, wherein said at least one forwarding
2 table entry further comprises:
3 a port identifier field, wherein
4 a port identifier stored in said port identifier field identifies a port.

1 114. The network device of claim 113, wherein
2 a security label stored in said label range field is associated with said port.

1 115. The network device of claim 113, wherein said at least one forwarding
2 table entry further comprises:
3 a media access control (MAC) address field; and
4 a virtual local area network (VLAN) identifier field, wherein
5 a combination of said MAC address field and said VLAN identifier
6 field are associated with said port identifier field and said label
7 range field.

1 116. The network device of claim 113, wherein
2 said media access control (MAC) address field is configured to store a MAC
3 address,
4 said VLAN identifier field is configured to store a VLAN identifier,
5 said VLAN identifier identifies a VLAN, and
6 a combination of said MAC address and said VLAN identifier identify said
7 port and said security label.

1 117. The network device of claim 114, wherein said at least one forwarding
2 table entry further comprises:
3 a media access control (MAC) address field configured to store a MAC
4 address, wherein

5 said MAC address is associated with a security label stored in said
6 label range field.

1 118. The network device of claim 112, wherein said at least one forwarding
2 table entry further comprises:

3 a virtual local area network (VLAN) identifier field, wherein
4 a VLAN identifier stored in said VLAN identifier field identifies a
5 VLAN, and
6 said VLAN is associated with a security label stored in said label range
7 field.